Notes on Galois Fields

Alireza Poostindouz

1 Basics

We start with some basic definitions and notions.

Definition 1 (Monoid) *Suppose that* S *is a set and operation '$\cdot$' is some binary operation* $\cdot : S \times S \mapsto S$*, called multiplication. Then* $(S, \cdot)$ *is a monoid if it satisfies the following axioms:*

1. ***(Closure)***
   S *is closed under multiplication, that is:*

$$a \cdot b \in S \qquad \forall a, b \in S$$

2. ***(Associativity)***

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall a, b, c \in S$$

3. ***(Identity element)***
   There exists an element e *in* S *such that*

$$a \cdot e = e \cdot a = a \qquad \forall a \in S$$

Example 1 *The set* $S = \{0, 1, 2, 3, 4, 5\}$ *with multiplication modulo* 6 *is a monoid. It has closure, associativity and the identity element is* 1*. For example you can see that* $4 \cdot 5 = 20 = 3 \times 6 + 2 = 2 \mod 6$ *and* 2 *belongs to* S*.*

Definition 2 (Group) *Suppose that* G *is a set and operation '$\cdot$' is some binary operation* $\cdot : G \times G \mapsto G$*, called multiplication. Then* $(G, \cdot)$ *is a group if it satisfies the following axioms:*

1. ***(Closure)***
   G *is closed under multiplication, that is:*

$$a \cdot b \in G \qquad \forall a, b \in G$$

2. ***(Associativity)***

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall a, b, c \in G$$

3. ***(Identity element)***
   There exists an element e *in* G *such that*

$$a \cdot e = e \cdot a = a \qquad \forall a \in G$$

4. ***(Inverse element)***
   For each a *in* G*, there exists an element* a^{-1} *in* G *such that*

$$a \cdot a^{-1} = a^{-1} \cdot a = e,$$

   where e *is the identity element.*

Example 2 *The set* $S = \{0, 1, 2, 3, 4, 5\}$ *with multiplication modulo* 6 *is not a group. It has closure, associativity and the identity element is* 1*. But for some elements the inverse does not exist. For example, there is no element* x *in* S *such that* $2 \cdot x = x \cdot 2 = 1 \mod 6$.

Example 3 *The set* $S = \{0, 1, 2, 3, 4, 5\}$ *with addition modulo* 6 *is a group. It has closure, associativity and the identity element is* 0*. And also for any element* x *in* S *the exist an "addition inverse", denoted by* $-x$ *such that* $x \cdot -x = x \cdot -x = 0 \mod 6$*. For example, addition inverse of* 1 *is* 5 *as* $1 + 5 = 6 = 0 \mod 6$*, or the addition inverse of* 2 *is* 4 *as* $2 + 4 = 0 \mod 6$.

Example 4 *For any prime number* p*, the set* $\{1, 2, 3, \ldots, p - 1\}$ *forms a group with multiplication modulo* p*. For example, for* $p = 5$*, the inverse of* 3 *is* 2*, as* $3 \cdot 2 = 1 \mod 5$*. Note that if we include* 0 *in the set, then we cannot find an inverse for* 0.

Definition 3 (Abelian Group) *Suppose that* G *is a set and operation '*$\cdot$*' is some binary operation* $\cdot : G \times G \mapsto G$*, called multiplication. Then* $(G, \cdot)$ *is an abelian group (commutative group) if it satisfies the following axioms:*

1. ***(Closure)***
   G *is closed under multiplication, that is:*

$$a \cdot b \in G \qquad \forall a, b \in G$$

2. ***(Associativity)***

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall a, b, c \in G$$

3. ***(Identity element)***
   There exists an element e *in* G *such that*

$$a \cdot e = e \cdot a = a \qquad \forall a \in G$$

4. ***(Inverse element)***
   For each a *in* G*, there exists an element* a^{-1} *in* G *such that*

$$a \cdot a^{-1} = a^{-1} \cdot a = e,$$

   where e *is the identity element.*

5. ***(Commutativity)***

$$a \cdot b = b \cdot a \qquad \forall a, b \in G$$

Example 5 *The set* $S = \{0, 1, 2, 3, 4, 5\}$ *with addition modulo* 6 *is also an abelian group.*

Definition 4 (Ring) *Suppose that* R *is a set and 2 binary operations, multiplication, '*$\cdot$*', and addition, '*$+$*', are defined. Then* $(R, +, \cdot)$ *is a ring if it satisfies the following axioms:*

1. R *is an abelian group under addition.*

2. R *is a monoid under multiplication.*

3. *Multiplication is distributive with respect to addition. That is*

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \qquad \forall a, b, c \in R \qquad \textbf{\textit{(left distributivity)}} \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \qquad \forall a, b, c \in R \qquad \textbf{\textit{(right distributivity)}}. \end{aligned}$$

Example 6 *The set* $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ *with addition and multiplication modulo* n *forms a ring. In fact it is a commutative ring as* $a \cdot b = b \cdot a$ *for any* $a, b \in \mathbb{Z}/n\mathbb{Z}$*.*

Definition 5 (Field) *Let* F *be a set with 2 binary operations, multiplication, '*$\cdot$*', and addition, '*$+$*'. Then* $(F, +, \cdot)$ *forms a field if the following conditions hold:*

1. $(F, +, \cdot)$ *is a ring.*

2. $(F \backslash \{0\}, \cdot)$ *is an abelian (commutative) group, where* 0 *is the additive identity.*

Note that commonly for a given finite field $(F, +, \cdot)$ with 0 as its additive identity, we call $(F, +)$ the "*additive group*" and $(F \backslash \{0\}, \cdot)$ the "*multiplicative group*" of F.

Theorem 1 *If* p *is a prime, then* $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ *is a field.*

It is very easy to see that $\mathbb{Z}/p\mathbb{Z}$ with addition and multiplication modulo p will form a field. Conventionally if a field is finite with p elements we denote it with $\mathbb{F}_p$ or $\mathbb{GF}(p)$ (Galois Field).

Example 7 ($\mathbb{GF}(2)$**)** *The simplest example would be* $\mathbb{GF}(2)$ *where the elements are from* $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ *and the addition and multiplication are done modulo* 2*. In this case, the addition is in fact the* XOR *operation and the multiplication is the* AND *operation.*

Below, you can see the addition and multiplication tables for $\mathbb{GF}(2)$*. The addition identity here is* 0 *as* $0 + \mathfrak{x} = 0 + \mathfrak{x} = \mathfrak{x} \mod 2$ *for all* $\mathfrak{x} \in \mathbb{Z}/2\mathbb{Z}$*. Also, it is easy to see that the multiplication identity (unit element) is* 1*, as* $1 \cdot \mathfrak{x} = \mathfrak{x} \cdot 1 = \mathfrak{x} \mod 2$ *for all* $\mathfrak{x} \in \mathbb{Z}/2\mathbb{Z}$*.*

Modulo 2 addition			Modulo 2 multiplication		
$+$	0	1	$\cdot$	0	1
0	0	1	0	0	0
1	1	0	1	0	1

Table 1: Addition and multiplication tables for $\mathbb{GF}(2)$.

Note that in $\mathbb{GF}(2)$ *we have*

- $-0 = 0$ *(addition inverse)*
- $-1 = 1$ *(addition inverse)*
- $1^{-1} = 1$ *(multiplication inverse)*

and remember that 0 *(the addition identity) does not have a multiplication inverse in any finite field.*

Example 8 ($\mathbb{GF}(3)$**)** *Another simple example is* $\mathbb{GF}(3)$ *where the elements are from* $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ *and the addition and multiplication are done modulo* 3*.*

Below, you can see the addition and multiplication tables for $\mathbb{GF}(3)$*. The addition identity here is* 0 *as* $0 + \mathfrak{x} = 0 + \mathfrak{x} = \mathfrak{x} \mod 3$ *for all* $\mathfrak{x} \in \mathbb{Z}/3\mathbb{Z}$*. Also, it is easy to see that the multiplication identity (unit element) is* 1*, as* $1 \cdot \mathfrak{x} = \mathfrak{x} \cdot 1 = \mathfrak{x} \mod 3$ *for all* $\mathfrak{x} \in \mathbb{Z}/3\mathbb{Z}$*.*

Modulo 3 addition				Modulo 3 multiplication			
$+$	0	1	2	$\cdot$	0	1	2
0	0	1	2	0	0	0	0
1	1	2	0	1	0	1	2
2	2	0	1	2	0	2	1

Table 2: Addition and multiplication tables for $\mathbb{GF}(3)$.

Note that in $\mathbb{GF}(3)$ *we have*

- $-0 = 0$ *(addition inverse)*
- $-1 = 2$ *(addition inverse)*
- $-2 = 1$ *(addition inverse)*
- $1^{-1} = 1$ *(multiplication inverse)*
- $2^{-1} = 2$ *(multiplication inverse)*

Example 9 ($\mathbb{GF}(5)$) *To construct* $\mathbb{GF}(5)$ *we use* $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ *and addition and multiplication modulo* 5*. Below, you can see the addition and multiplication tables for* $\mathbb{GF}(5)$*.*

Modulo 5 addition						Modulo 5 multiplication					
$+$	0	1	2	3	4	$\cdot$	0	1	2	3	4
0	0	1	2	3	4	0	0	0	0	0	0
1	1	2	3	4	0	1	0	1	2	3	4
2	2	3	4	0	1	2	0	2	4	1	3
3	3	4	0	1	2	3	0	3	1	4	2
4	4	0	1	2	3	4	0	4	3	2	1

Here, we can see that $-\mathtt{x} = 5 - \mathtt{x}$ for $\mathtt{x} \in \mathbb{Z}/5\mathbb{Z}$. For example, $-2 = 3$. Also, based on the multiplication table we can find the multiplication inverse, such as $1^{-1} = 1$ and $2^{-1} = 3$.

1.1 Primitive Element

Definition 6 *Let* $\mathtt{x}$ *be an element of* $\mathbb{GF}(\mathtt{p})$*. Then the order of* $\mathtt{x}$ *is the smallest positive integer* $\mathtt{k}$ *such that* $\mathtt{x}^{\mathtt{k}} = 1$*, where* 1 *is the multiplication identity (unit element).*

Theorem 2 *Let* $\mathtt{x}$ *be an element of* $\mathbb{GF}(\mathtt{p})$ *and* $\mathtt{x}$ *is not the addition identity (*$\mathtt{x} \neq 0$*). If* $\mathtt{k}$ *is the order of* $\mathtt{x}$*, then* $\mathtt{k}$ *divides* $\mathtt{p} - 1$*.*

Example 10 *Consider* $\mathbb{GF}(5) = \{0, 1, 2, 3, 4\}$*. Let's find the order of* 2*. Using example 5 we can easily see that:*

$$2 \times 2 = 4,$$
$$4 \times 2 = 3,$$
$$3 \times 2 = 1.$$

Meaning that the smallest $\mathtt{k}$ *such that* $2^{\mathtt{k}} = 1$ *is* 4*, i.e.* $\mathtt{order}(2) = 4$*. Now let's find the order of* 4*. As* $4 \times 4 = 1$*, we simple see that* $\mathtt{order}(4) = 2$*.*

Theorem 3 (Primitive Element) *Every* $\mathbb{GF}(p)$ *has at least one element* α *with order* $(p-1)$*, i.e.* $\alpha^{(p-1)} = 1$*, where* 1 *is the unit element. In other words* α *is the primitive* $(p-1)$*−th root of unity.*

Example 11 *As we saw in the previous example we now know that for* $\mathbb{GF}(5)$*,* 2 *is a primitive element as* $\mathtt{order}(2) = 4$*.*

Definition 7 *Let* $(G, \cdot)$ *be a group. We say that* $x \in G$ *is a generator for* G *if*

$$\{x^j \quad \forall j \in \mathbb{N}\} = G.$$

Remark 8 *If* α *is a primitive element for* $\mathbb{GF}(p)$ *then* α *is a generator for the multiplicative group of* $\mathbb{GF}(p)$*. That is*

$$\{\alpha^j \quad \forall j \in \mathbb{N}\} = \mathbb{GF}(p) \setminus \{0\},$$

where 0 *is the addition identity. If* p *is a prime number, then*

$$\{\alpha^j \quad \forall j \in \mathbb{N}\} = \{1, 2, \ldots, p-1\}.$$

Example 12 *We know that for* $\mathbb{GF}(5)$*,* 2 *is a primitive element. Now we observe that:*

$$\begin{aligned}\{2^j \quad \forall j \in \mathbb{N}\} &= \{2,\ 2\times 2,\ 2\times 2\times 2,\ 2\times 2\times 2\times 2,\ \cdots\} \\ &= \{2, 4, 3, 1\} = \mathbb{GF}(5) \setminus \{0\}.\end{aligned}$$

Remember that $(\mathbb{GF}(5) \setminus \{0\}, \cdot)$ *is the multiplicative group of* $\mathbb{GF}(5)$ *and the above observation proves that* 2 *is a generator for the multiplicative group of* $\mathbb{GF}(5)$*. Also we know that* 4 *is not a primitive element and so:*

$$\begin{aligned}\{4^j \quad \forall j \in \mathbb{N}\} &= \{4,\ 4\times 4,\ 4\times 4\times 4,\ 4\times 4\times 4\times 4,\ \cdots\} \\ &= \{4, 1\} \neq \mathbb{GF}(5) \setminus \{0\}.\end{aligned}$$

Theorem 4 *For any finite field with* n *elements,* n *is either a prime or a prime power.*

Example 13 *For* $n = 6$ *there does not exist any* $\mathbb{GF}(6)$*. For instance, take* $\{0, 1, \ldots, 5\}$ *and modulo* 6 *arithmetics. There does not exist an inverse for* 2*; therefore, we could not find a construction for* $\mathbb{GF}(6)$ *and no such thing exists.*

Example 14 *For* $n = 8$ *there exists a construction for a finite field. But, in this case the set* $\{0, 1, \ldots, 8\}$ *and modulo* 8 *arithmetics would not work! One can easily see that, for example, the inverse of* 4 *does not exist. To find out how to construct* $\mathbb{GF}(8)$ *we need to learn more about Galois Fields.*

2 Field Extensions (Construction of $\mathbb{GF}(p^m)$)

To construct a Galois field $\mathbb{GF}(p^m)$ we need to use the notion of vector spaces and use polynomial arithmetics as well.

Definition 9 (Vector Space) *A set V is a vector space over a field F if 2 binary operations "vector addition", '$+ : V \times V \mapsto V$', and "scalar multiplication", '$\cdot : F \times V \mapsto V$' are defined and the following axioms are satisfied:*

1. *V is a commutative (abelian) group under vector addition.*
2. *V is closed under scalar multiplication.*
3. $a \cdot (b \cdot v) = (a \cdot b) \cdot v \qquad \forall a, b \in F, \forall v \in V$
4. $a \cdot (u + v) = a \cdot u + a \cdot v \qquad \forall a \in F, \forall u, v \in V$
5. $(a + b) \cdot v = a \cdot v + b \cdot v \qquad \forall a, b \in F, \forall v \in V$
6. $1 \cdot v = v \qquad \forall v \in V$, *where* 1 *is the multiplication identity of* F.

Example 15 *For example let's define a vector space with dimension* 2 *over* $\mathbb{GF}(5)$. *We can denote each vector* $v \in V$ *by*

$$v = \begin{bmatrix} a_v \\ b_v \end{bmatrix} \qquad a_v, b_v \in \mathbb{GF}(5).$$

We can define the vector addition using the addition of $\mathbb{GF}(5)$ *(that is addition modulo 5) as the following. For* $v_1 = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}$ *and* $v_2 = \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}$ *the vector addition is defined as:*

$$v_1 + v_2 = \begin{bmatrix} a_1 + a_2 \\ b_1 + b_2 \end{bmatrix},$$

where in the expressions $a_1 + a_2$ *and* $b_1 + b_2$, *the addition,* $+$, *is the* $\mathbb{GF}(5)$ *addition.*

2.1 Polynomials Over Galois Fields

A polynomial P over $\mathbb{GF}(q)$ with degree n is of the following form

$$P = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

if all $a_j \in \mathbb{GF}(q)$ and $a_n \neq 0$ where 0 is the fields addition identity.

2.1.1 Galois Field Arithmetics of Polynomials

Definition 10 *The* ***addition*** *of two polynomials* $P_1 = a_0 + a_1x + a_2x^2 + \cdots + a_nx^m$ *and* $P_2 = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ *over* $\mathbb{GF}(q)$ *is*

$$P_1 + P_2 = \sum_{j}^{\max(m,n)} (a_j + b_j)x^j.$$

Note that obviously the addition in expression $(a_j + b_j)$ *is the addition of* $\mathbb{GF}(q)$.

Example 16 *Consider the following two polynomials defined over* $\mathbb{GF}(5)$.

$$P_1 = x^7 + 3x^2 + x$$
$$P_2 = 4x^6 + 2x^2 + x$$

Then we have

$$\begin{aligned} P_1 + P_2 &= x^7 + 3x^2 + x + 4x^6 + 2x^2 + x \\ &= x^7 + 4x^6 + (3+2)x^2 + (1+1)x \\ &= x^7 + 4x^6 + 2x. \end{aligned}$$

Note that in the last step we used the fact that $3 + 2 = 0 \mod 5$.

Definition 11 *The* ***subtraction*** *of two polynomials* $P_1 = a_0 + a_1x + a_2x^2 + \cdots + a_nx^m$ *and* $P_2 = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ *over* $\mathbb{GF}(q)$ *is*

$$P_1 - P_2 = P_1 + P_2',$$

where P_2' *is*

$$P_2' = (-b_0) + (-b_1)x + (-b_2)x^2 + \cdots + (-b_n)x^n$$

with $-b_j$ *denotes the additive inverse of* b_j.

Example 17 *Consider the following two polynomials defined over* $\mathbb{GF}(5)$.

$$P_1 = x^7 + 3x^2 + x$$
$$P_2 = 4x^6 + 2x^2 + x$$

Then for $P_1 - P_2$ *we have*

$$\begin{aligned} P_1 - P_2 &= x^7 + 3x^2 + x + (-4)x^6 + (-2)x^2 + (-1)x \\ &= x^7 + 3x^2 + x + (1)x^6 + (3)x^2 + (4)x \\ &= x^7 + x^6 + 4x^2. \end{aligned}$$

Remark 12 *Note that for polynomials over* $\mathbb{GF}(2)$ *the addition and subtraction are identical as the addition and subtraction over* $\mathbb{GF}(2)$ *are both the same as an* XOR *operation.*

Definition 13 *The* ***multiplication*** *of two polynomials* $P_1 = a_0 + a_1x + a_2x^2 + \cdots + a_nx^m$ *and* $P_2 = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ *over* $\mathbb{GF}(q)$ *is*

$$P_1P_2 = \sum_j \sum_k (a_j \cdot a_k)x^{j+k}.$$

Note that the addition in exponent x^{j+k} *is the standard integer addition but the multiplication in* $(a_j \cdot a_k)$ *is the multiplication of* $\mathbb{GF}(q)$.

Example 18 *Consider the following two polynomials defined over* $\mathbb{GF}(2)$.

$$P_1 = x^7 + x^2 + x$$
$$P_2 = x^6 + x^2 + 1$$

then

$$\begin{aligned} P_1P_2 &= \left(x^7 + x^2 + x\right)\left(x^6 + x^2 + 1\right) \\ &= x^{13} + x^9 + x^7 + x^8 + x^4 + x^2 + x^7 + x^3 + x \\ &= x^{13} + x^9 + x^8 + x^4 + x^3 + x^2 + x. \end{aligned}$$

Note that $1 + 1 = 0$ *in* $\mathbb{GF}(2)$ *thus* $x^7 + x^7 = 0$.

Definition 14 *Consider two polynomials* $P_1 = a_0 + a_1x + a_2x^2 + \cdots + a_nx^m$ *and* $P_2 = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ *over* $\mathbb{GF}(q)$. *Then there are unique polynomials* Q *and* R *over* $\mathbb{GF}(q)$ *such that:*

$$P_1 = QP_2 + R,$$

and we call Q *the quotient and* R *remainder of dividing* P_1 *by* P_2. *Also* P_1 *is called the dividend and* P_2 *is the divisor.*

Example 19 *The answer to* $(x^5 + x^3 + x^2 + x) \div (x^4 + x^3 + 1)$ *is*

$$x^5 + x^3 + x^2 + x = (x^4 + x^3 + 1)(x + 1) + (x^2 + x)$$

Here $(x + 1)$ *is the quotient and* $(x^2 + x)$ *is the remainder.* [1]

If the remainder R in $P_1 \div P_2$ is zero, then we say P_1 is divisible by P_2; or equivalently we say P_2 is a factor of P_1.

Definition 15 (Irreducible Polynomial) *A polynomial* P *of degree* m *defined over some field* $\mathbb{GF}(q)$ *is called irreducible if* P *has no divisor polynomials in* $\mathbb{GF}(q)$ *with degree less than* m.

Definition 16 (Primitive Polynomials) *content...*

[1] To learn how to do the polynomial long divisor watch the following video : `https://www.youtube.com/watch?v=H94ma2ofGuc`.

2.1.2 Construction of $\mathbb{GF}(2^3)$ from $\mathbb{GF}(2)$

With the current knowledge that we have, let's try to design a valid construction for $\mathbb{GF}(8)$. We have already observed that the set $\mathbb{Z}/8\mathbb{Z} = \{0, 1, \ldots, 7\}$ together with modulo 8 arithmetics cannot construct a finite field. (See Example 14). It is very easy to see that simply defining a vector space of dimension 3 over $\mathbb{GF}(2)$, i.e. $\nu = (a_0, a_1, a_2)$ with $a_j \in \mathbb{GF}(2)$, together with element–wise binary addition and multiplication will not be enough for constructing a finite field over 8 elements.

But, we can use polynomials of degree at most $2 = 3-1$ with coefficients of any polynomial being elements of a corresponding vector $\nu = (a_0, a_1, a_2) \in \mathbb{GF}(2)^3$.

#	$a_0 + a_1x + a_2x^2$	(a_0, a_1, a_1)		
P_0	0	0	0	0
P_1	1	1	0	0
P_2	x	0	1	0
P_3	$x + 1$	1	1	0
P_4	x^2	0	0	1
P_5	$x^2 + 1$	1	0	1
P_6	$x^2 + x$	0	1	1
P_7	$x^2 + x + 1$	1	1	1

Table 3: Defining tentative elements for $\mathbb{GF}(8)$ using polynomials.

Now we have to see if polynomial arithmetics together with the set $F = \{P_0, P_1, \ldots, P_7\}$, defined in the table above, can actually construct a finite field.

Addition: For addition we are lucky and we can solely use the polynomial addition. As we can see, the polynomial addition together with F will create an abelian group $(F, +)$. For example:

$$\begin{aligned} P_2 + P_3 &= (x) + (x + 1) \\ &= 1 = P_1. \end{aligned}$$

Or

$$\begin{aligned} P_5 + P_3 &= (x^2 + 1) + (x + 1) \\ &= x^2 + x = P_6. \end{aligned}$$

Multiplication: As for the multiplication it might seem in the first glance that using solely the polynomial multiplication will give us closure and all group properties we need for the multiplicative group. For example:

$$\begin{aligned} P_2P_3 &= (x)(x + 1) \\ &= x^2 + x = P_6. \end{aligned}$$

But soon we realize that this will not give us closure! For instance:

$$\begin{aligned} P_4 P_5 &= (x^2)(x^2+1) \\ &= x^4 + x^2 \notin F. \end{aligned}$$

So to resolve this problem we need to use a polynomial P^* of order 3 and then for the field multiplication "$P_j \cdot P_k$", we would take the remainder of $(P_j P_k) \div P^*$. Now this special polynomial P^* cannot be just any polynomial, it has to be an irreducible and in fact a primitive polynomial of degree 3. Thus, rigorously speaking we can define the field multiplication as follows. For each P_j and P_k in F

$$P_j \cdot P_k = \text{Remainder}\left[(P_j P_k) \div P^*\right],$$

where P^* is a primitive polynomial of degree 3 over $\mathbb{GF}(2)$. Note that $P_j \cdot P_k$ denotes the field multiplication and $(P_j P_k)$ is the standard polynomial multiplication over $\mathbb{GF}(2)$.

Now let's take $P^* = x^3 + x + 1$, which is a primitive polynomial over $\mathbb{GF}(2)$. Now for the field multiplication we defined as above and the set $F\backslash\{0\}$ we get the abelian multiplicative group. For example consider the same multiplication we tried last time:

$$\begin{aligned} P_4 \cdot P_5 &= \text{Remainder}\left[(x^2)(x^2+1) \div P^*\right] \\ &= \text{Remainder}\left[(x^4 + x^2) \div (x^3 + x + 1)\right] \\ &= x = P_2 \in F. \end{aligned}$$

Therefore, we have successfully constructed out new field $\mathbb{GF}(8)$ based on a vector spaced defined with polynomials over $\mathbb{GF}(2)$ and some specific polynomial arithmetics.

Now to find the primitive element of $F = \mathbb{GF}(8)$ we need to find a polynomial $P_\alpha \in F$ such that

$$\{P_\alpha^j \quad \forall j \in \mathbb{N}\} = F\backslash\{0\}.$$

Easily we can observe that for $P_\alpha = P_2 = x$ we get:

$$\begin{aligned} \{P_2^j \quad \forall j \in \mathbb{N}\} &= \{x, (x)\cdot(x), (x)\cdot(x)\cdot(x), (x)\cdot(x)\cdot(x)\cdot(x), \cdots\} \\ &= \{x, x^2, x+1, x^2+x, x^2+x+1, x^2+1, 1\} \\ &= F\backslash\{0\}. \end{aligned}$$

So we can have our construction table for $\mathbb{GF}(8)$ as the following:

#	α^j	$a_0 + a_1x + a_2x^2$	(a_0, a_1, a_1)		
P_0	0	0	0	0	0
P_1	α^7	1	1	0	0
P_2	α^1	x	0	1	0
P_3	α^3	$x + 1$	1	1	0
P_4	α^2	x^2	0	0	1
P_5	α^6	$x^2 + 1$	1	0	1
P_6	α^4	$x^2 + x$	0	1	1
P_7	α^5	$x^2 + x + 1$	1	1	1

Table 4: Defining tentative elements for $\mathbb{GF}(8)$ using polynomials.

References

[1] Rao, K. Deergha. *Channel coding techniques for wireless communications.* Springer, 2015.

[2] Van Lint, Jacobus Hendricus. *Introduction to coding theory.* Vol. 86. Springer Science & Business Media, 2012.